Program Management Study

Department of Defense Critical Infrastructure Protection Program

Defining Roles and Functions for the Future

Prepared for the Joint Staff (J5)
Homeland Security Division

July 2003

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department of Defense Critical Infrastructure Protection Program. Defining Roles and Functions for the Future	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense,Joint Staff (J5),Washington,DC,20301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

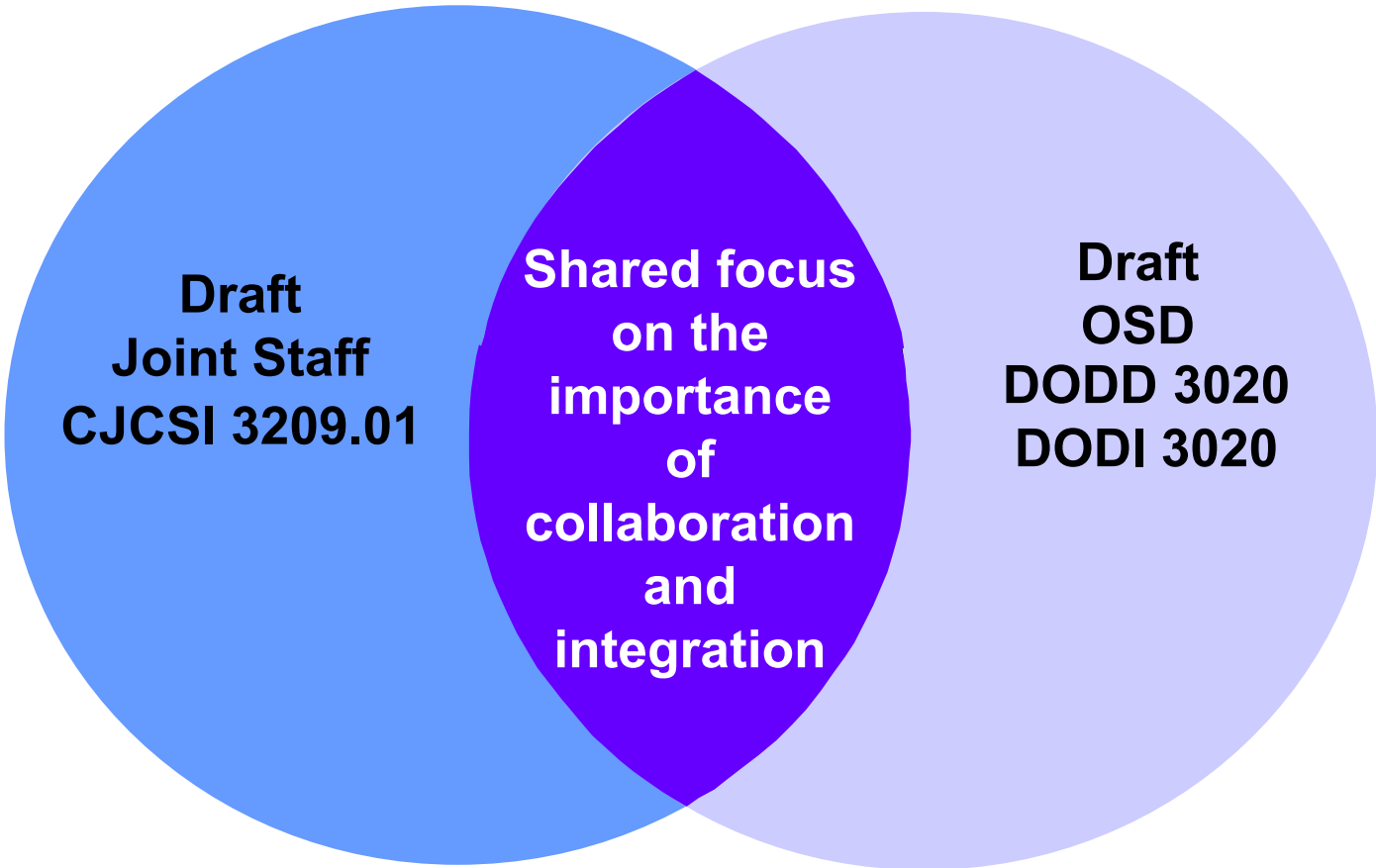
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**38**	

Overview

- Background
- Current CIP Landscape
- Key Roles and Functions
  - Policy and Oversight
  - Resources "Honest Broker"
  - Technology
  - Analysis & Integration
  - Outreach & Awareness
  - Risk Management
- Program Management Options
  - Executive Agent (EA)
  - CIP Field Activity (CIPFA)
  - Joint Staff OPR (OPR)
  - Combined Option

The Joint Staff (J5) chartered an independent assessment to recommend program management options for the DoD CIP Program. The study was conducted at the request of the Joint Staff because of a shared belief by both J5 and the DOD CIP Director that the time was right for considering a DoD-wide CIP Program Office.



Organizational options were proposed for consideration at the onset of the study.

1. Designation of an Executive Agent (EA) for CIP within OSD
2. Creation of a CIP Joint Program Office staffed by JPO-STC
3. Creation of a Joint Staff Task Force for CIP

Over the course of the study those options were modified to the following:

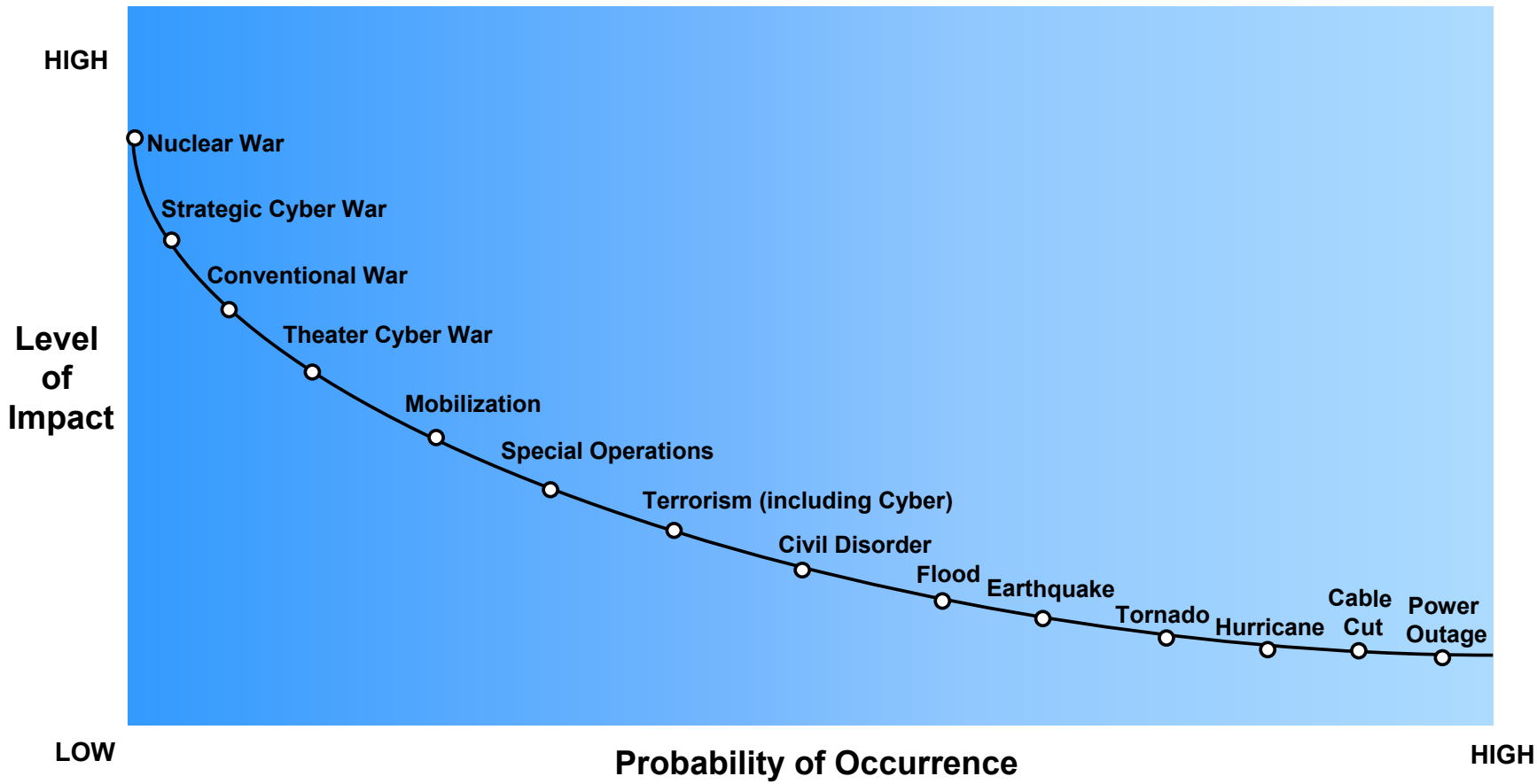
1. Formal Designation of an Executive Agent and creation of a CIP Program Management Office within OSD
2. Creation of a DOD CIP Field Activity with JPO-STC providing technical support
3. Designation of an Office of Primary Responsibility (OPR) within the Joint Staff for Mission Assurance/CIP
4. Creation of a program management model combining all or some of the proposed options

The study is based on an understanding that the following conditions are required for an effective DOD CIP Program.

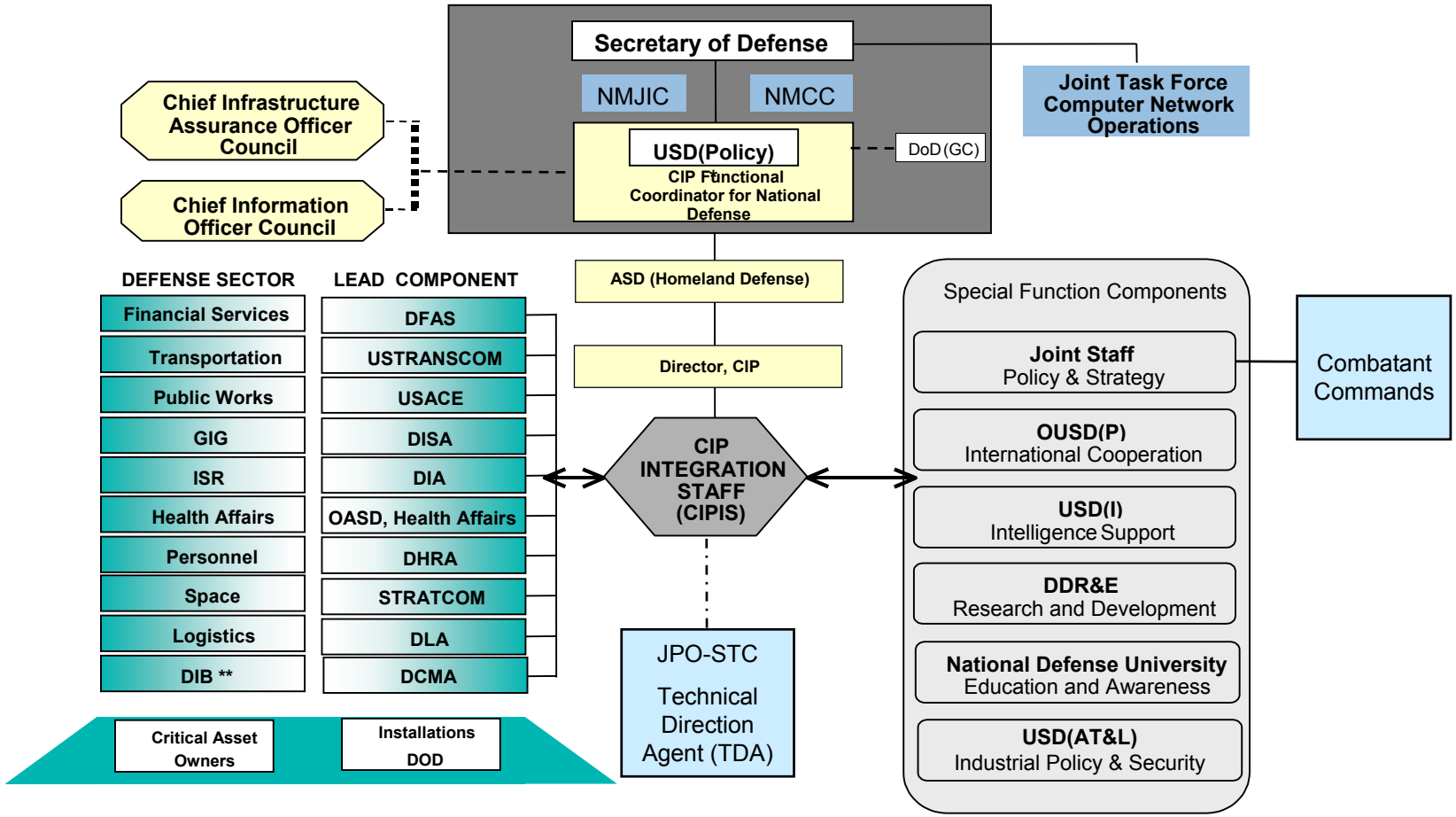
- There continues to be a Program Management Office for DOD CIP.
- Approved and exercised DOD Directives and Instructions exist that clearly explain the roles and responsibilities of DOD CIP elements.
- The DOD CIP arena includes representation and active participation from Commands, Services, and Agencies, as well as OSD and the Joint Staff.
- Coordinated technical direction is provided to CIP stakeholders and standard approaches are implemented for asset analysis and assessment (e.g., asset criticality assessments, dependency assessments, vulnerability assessments).
- An effective CIP I&W system and capability are established to ensure the timely receipt and coordination of threat information related to potential critical infrastructure attacks and disruptions.
- Resources are available to meet all DOD CIP operational, technology, and R&D requirements.

DOD CIP focuses on "mission assurance" and encompasses a broad spectrum of threats ranging from cable cuts to power outages to nuclear war.

CIP THREAT SPECTRUM



The existing DoD CIP program landscape consists of loosely defined lines of coordination between the Combatant Commanders, the Joint Staff, OSD, and the rest of the community. The Combatant Commanders, in particular are disconnected from the CIP Community. As the ultimate users of service and agency-owned assets, Combatant Commands must be well integrated in the CIP program.



*** Defense Industrial Base*

** Location of CIP Program Management responsibilities to be determined.*

Based on observation and inputs from key stakeholders, several broad themes emerged that characterize the current state of the DoD CIP Program:

- There are a large number of Government and industry organizations playing in the DoD CIP Program with varying degrees of effectiveness.
- Although the roles in the CIP arena will be well defined once the draft DOD Directive 3020, DOD Instruction 3020, and CJCSI 3209.01 are promulgated, the specific functions within those roles are not well defined.
- The focal points for CIP information sharing face barriers in coordination due to current stovepipe organizational structure.
- Although efforts are in progress, there is still limited coordination across DoD infrastructure sectors in terms of conducting interdependency analyses between the sectors.
- The Government's difficulties in resolving budgetary problems and barriers to information sharing, and its failure to make a "business case" for CIP have caused some key players to take a "wait and see" approach.
- Lack of trust remains a major impediment to information sharing - within Government, within industry, and between Government and industry.
- The current bureaucratic culture is not conducive to responding to a rapidly changing environment.

There are a number of key programmatic challenges that prevent the current CIP program from being prepared to meet the rapid changes of the future.

- Limited organizational resources exist to implement an effective program that assures critical infrastructures are protected consistent with the National Military Strategy.
- The current DOD CIP Strategic Plan and other guidance lack the specificity required to implement the program.
- A collaborative systems architecture and technology infrastructure need to be developed for a community-wide CIP program.
- Connectivity and access remain a barrier to effective information sharing.
- Commands, Services and Agencies are in the initial stages of organizing their CIP Programs and their ability to sustain them is dependent on resources.
- The CIP community is having a difficult time ensuring that new technologies are effectively transitioned into product-oriented CIP practices that support the National Security Strategy.

- No asset characterization standards have been provided to the sector members.
- A consolidated catalog of vulnerability assessment data is planned, but has not yet been established for the community.
- No comprehensive vulnerability assessment process based on community-wide standards has been established.
- No mutually agreed upon core competencies or certification process exists for key skills required to assess and remediate critical vulnerabilities.
- Prioritization of remediation requirements is determined by asset owners with limited input from the asset users.
- Classification guidance for DOD CIP program needs to be reviewed.
- No coordinated process exists to ensure CIP program participants are trained on current policies and policy changes.

The implementation of study recommendations will depend on the answers to several important questions.

- How will the following organizational changes currently taking place impact the DOD CIP Program roles and functions?*
  - Establishment of the new Department of Homeland Security (DHS)
  - Establishment of ASD/Homeland Defense (HD)
  - Establishment of a new USD for Intelligence
  - The stand up of NORTHCOM
- Will adequate funding be available to support DOD CIP Program requirements separate from the current Antiterrorism (AT), Force Protection (FP), Continuity of Operations (COOP), Readiness, and Information Assurance (IA) program funds?

**Assumptions associated with these organizational changes are reflected on page 5.*

Closing the gaps between the current and desired future state for CIP requires broad participation and offers an opportunity for key stakeholders to assume a larger role in the Program.

Gaps

Policy & Oversight

Resources

Technology

Analysis & Integration

Outreach & Awareness

Risk Management

- **THE POLICY & OVERSIGHT GAP** -A new DOD directive and instruction that adequately explain the roles and responsibilities of all DOD CIP elements and how they operate together need to be promulgated. Stakeholders perceive a lack of leadership and oversight in terms of ensuring a results-oriented, integrated CIP program.
- **THE RESOURCE GAP -** In order to meet the policy, technical, and operational requirements of the desired future DOD CIP state, staff resources must be acquired.
- **THE TECHNOLOGY GAP –** Steps must be taken to complete the develop of a standard architecture and collaborative technological environment to do analysis, warning, and prediction. Despite a large investment, the technology is not yet operational or able to meet the needs of the sectors and commands.
- **THE ANALYSIS & INTEGRATION GAP -** Steps must be taken to develop a capability that ensures that the right information is collected, analyzed and shared among DOD CIP participants.
- **THE OUTREACH & AWARENESS GAP -** To best protect the defense infrastructure from attacks along the crisis spectrum, there must be broad and active participation and integration of information from both the DIB and commercial industry in DOD CIP activities. Additionally, international-level cooperation and information exchange must take place. To ensure an effective flow of information between Government,industry and international partners, a trust relationship must develop beyond what exists now.
- **THE RISK MANAGEMENT GAP -** Coordinated risk mitigation, incident response, and contingency plans and capabilities that do not currently exist must be developed and exercised to effectively respond to attacks and restore the affected infrastructure.

Based on an assessment of key functions and gaps, the study team identified six primary roles that need to be assigned.

KEY ROLES
" DOD CIP Program Director" with policy and oversight responsibilities
"Honest Broker" between the sectors, commands, services and agencies responsible for resource requirements prioritization and financial management
"Technical Direction Lead" responsible for research and development of CIP tools and technology standards that can be used to aggregate and analyze asset data, facilitate inter-dependency analyses and integrate data across the Defense Infrastructures
"Analysis and Integration Lead" responsible for coordinating and conducting analyses and assessments of threats and vulnerabilities to critical infrastructures, and integrating data across the Defense Infrastructures, Defense Industrial Base (DIB) and Commercial sector
"Outreach & Awareness Lead" serving as focal point for Government and Industry, Domestic and International DOD CIP awareness, information sharing and training
"Risk Management Lead" responsible for monitoring planning efforts for risk mitigation, incident response, and reconstitution of DoD Critical Infrastructures

ROLE: "DOD CIP Program Director" with policy and oversight responsibilities

Key Functions:

- Oversee development and implementation of DOD Directives and Instructions for CIP throughout the Department to ensure all DoD Components are complying.(J5*)
- Conduct an annual review of the DoD Critical Infrastructure Protection Program to ensure the Department is meeting its goals and objectives.(J5*)
- Ensure the Critical Infrastructure Protection Program is incorporated into the DoD Planning, Programming, Budgeting & Execution System (PPBES) process.(J8*)
- Establish Department-wide information classification, release, and special handling instructions for the DoD Critical Infrastructure Protection Program.(J2*)
- Ensure relevant legal issues, as well as proprietary protection, counterintelligence, and law enforcement issues are addressed fully in support of DoD Critical Infrastructure Protection Program goals and objectives.(J2/J5*)
- Oversee application of a standard methodology for identifying the critical domestic and foreign infrastructure assets the Department relies upon to fulfill its homeland defense and force projection responsibilities. (J3*)
- Oversee development and maintenance of a distributed database that will serve as the master DoD repository for all critical infrastructure asset and interdependency related information. (J3*)
- Ensure present and projected indications and warning networks are used to submit operational status reports on the viability of every identified critical infrastructure asset and their interdependent potential points of failure.(J2*)
- Ensure effective physical and cyber vulnerability assessment policies and procedures are developed and implemented fully throughout the Department.(J5/J3/J6*)
- Ensure a sufficient number of adequately trained personnel are available to execute the DoD Critical Infrastructure Protection Program.(J1*)
- Oversee the Department's Critical Infrastructure Protection related training and awareness program initiatives.(J7*)
- Provide guidance on and maintain cognizance of DoD Critical Infrastructure Protection Program related mitigation and remediation activities.(J3*)

Joint Staff Support to OSD Function

ROLE: "Honest Broker" between the sectors, commands, services and agencies with resource requirements prioritization and financial management responsibilities

Key Functions:

- Develop and maintain the CIP financial baseline. (J8*)
- Develop Program Objective Memorandum (POM) analysis process to streamline DoD CIP PPBES Programming Phase processes, enable collaborative development, adequately characterize requirements and balance resources across the DOD CIP enterprise in real time IAW planning guidance. (J8*)
- Implement common Work Breakdown Structure (WBS) and Financial Management (FM) tool set to capture, understand and control cost and enable automated linkage of the POM and Budgeting Phases. Implement financial and cost metrics to measure performance against benchmarks. (J8*)
- Perform analyses of DOD CIP POM requirements, capabilities and resources to develop set of POM issues that efficiently resource existing DoD CIP program requirements and suitably justify unfunded items. (J8*)
- Develop CIP input to the Defense Planning Guidance (DPG) (J5/J8*)
- Develop budget issues and perform trend analysis for the DoD CIP Program in support of OSD and President's Budget Estimate Submission development. (J8*)
- Recommend alternative mechanisms for funding DoD CIP initiatives which benefit multiple Federal departments, agencies, and entities. (J8*)
- Identify appropriate levels of funding for budget submissions to support DoD CIP requirements. (J8*)

Joint Staff Support to OSD Function

ROLE: "Technical Direction Agent" responsible for research and development of CIP tools and technology standards that can be used to aggregate and analyze asset data, facilitate inter-dependency analyses, and integrate threat and vulnerability data across the Defense Infrastructures.

Key Functions:

- Develop a standard, customer friendly methodology for identifying the critical domestic and foreign infrastructure assets the Department relies upon to fulfill its homeland defense and force projection responsibilities. (J3/J6*)
- Develop analytical standards and procedures to permit effective, Department-wide, infrastructure support analyses and vulnerability assessments. (J3/J6*)
- Develop capability to provide the Secretary of Defense, Chairman of the Joint Chiefs of Staff, Military Departments, and Combatant Commands real time situational awareness of infrastructure assets designated as critical to U.S. military operations. (J3/J6*)
- Work with the Director, Defense Information Systems Agency to develop and maintain a network that allows real-time alerts and warnings CIP-wide, and that facilitates the routine sharing of information concerning risks to critical infrastructures.(J6/J2*)
- Work with the Director, National Imagery and Mapping Agency to support the DoD Critical Infrastructure Protection Program with the annotated imagery needed for the development of situational awareness and complex modeling and simulation visualization tools.(J6/J8*)

Joint Staff Support to OSD Function

ROLE: "Analysis and Integration Lead" responsible for coordinating and conducting analyses and assessments of threats and vulnerabilities to critical infrastructures, and integrating data across the Defense Infrastructures, DIB, and Commercial sector.

Key Functions:

- Facilitate cooperation and sharing of tools, techniques, and lessons learned across the Sectors, Commands, Services and Agencies (J5/J3/J6*)
- Work with DHS to establish a dialogue throughout the Federal and State governments to foster a common understanding of the interagency interdependencies. (J5*)
- Coordination with the appropriate DoD Components and with the permission of the owners, physical vulnerability assessments of designated DoD and non-DoD classified and unclassified critical infrastructures. (J3/J6*)
- Identify and map the interdependencies across all the critical infrastructures. (J3/J6*)
- Identify single points of failure across all relevant critical infrastructures (J3/J6*)
- Lead development of I&W methodology for DoD CIP (J2*)
- Coordinate threat intelligence support to DoD sectors, commands, services, and agencies (J2/J3*)
- Ensure that threat assessments on DoD infrastructures, systems, or assets are prepared and presented to appropriate CIP stakeholders (J2/J3*)
- In cooperation with the Counterintelligence Field Activity (CIFA), provide counter-intelligence support to the CIP leadership and organizations, in coordination with the Military Services (J2*)
- Coordinate all-source analysis and data fusion to generate CIP alerts and warnings for on-going events.(J2*)
- Contribute to identification of requirements and development of I&W predictive analysis tools.(J2/J6*)

Joint Staff Support to OSD Function

ROLE: "Outreach & Awareness Lead" serves as the DoD support focal point for Government and Industry, Domestic and International DOD CIP awareness, information sharing and training

Key Functions:

- In conjunction with the Department of Homeland Security (DHS) and the Department of State (DOS), elevate the awareness of and promote Critical Infrastructure Protection through a variety of activities, such as information sharing and cooperative agreements with the private sector, as well as other federal departments, state and local governments, and allied/friendly foreign governments as applicable. (J5*)
- In conjunction with the DHS and the DOS, facilitate the sharing of industry's sensitive information with the Government in a protected and trusted environment.(J4/J5*)
- Interface between government and industry to promote the sharing of classified information in a protected and trusted environment.(J2/J4*)
- Represent the DoD in Critical Infrastructure Protection related discussions and agreements with other U.S. Government, private sector officials, state and local governments, and allied/friendly foreign governments. (J5*)
- Work with the Under Secretary of Defense for Acquisition, Technology, and Logistics, to ensure its policies and assurance standards established as a result of Draft DoD Directive 3020 are integrated into all appropriate acquisition policy guidance. (J4*)
- Develop relationships with Federal departments and agencies as identified in Draft DOD Directive 3020. (J5/J3*)

Joint Staff Support to OSD Function

ROLE: "Risk Management Lead" responsible for overseeing planning efforts for risk mitigation, incident response, and reconstitution of DoD Critical Infrastructures

Key Functions:

- Provide guidance on and maintain cognizance of DoD Critical Infrastructure Protection Program related risk mitigation and remediation, response and reconstitution activities.(J3/J7*)
- Provide a framework that will enable DoD to monitor and manage the readiness posture of mission essential components of the critical infrastructures that D0D relies on.(J3*)
- Facilitate emergency response planning, training and exercises across all sectors.(J8/J3*)
- Work with the Director, National Security Agency to conduct or oversee, in coordination with the appropriate DoD Components and with the permission of the owners, cyber vulnerability assessments of designated DoD and non-DoD classified critical infrastructures. Require the Director, National Security Agency to conduct or oversee all actions that are necessary to increase the reliability, redundancy, protection, and restoration of classified information systems supporting DoD critical infrastructures.(Source: Draft DODD 3020) (J6*)
- Work with the Director, Defense Information Systems Agency to conduct or oversee all actions that are necessary to increase the reliability, redundancy, protection, and restoration of unclassified information systems supporting DoD critical infrastructure assets.(J6*)

Joint Staff Support to OSD Function

The Draft CJCSI 3209.01 assigns responsibilities to each of the Joint Staff functional areas.

J-1 Personnel

- Coordinates with C/S/As on CIP Personnel requirements
- Primary POC for interface w/ Personnel, Finance and Heath Affairs Sectors

J-2 Intelligence/I&W

- Lead for CIP Intel, CI, and I&W issues
- Primary POC for interface with with ISR Sector

J-3 Operations

- Coordinates with J codes on CIP vulnerabilities
- Coordinates with C/S/As on Force Protection Issues
- Primary POC for Joint Monthly Readiness Review, CIP CNO requirements, TRANSCOM, SPACE Sector, Mission Assurance Asset Database

J-4 Logistics

- Coordinates with C/S/As on Logistics requirements
- Primary POC for interface w/ Logistics, Transportation, Public Works Sectors

J-5 Policy/Strategy

- Lead for coordinating strategic CIP policy issues
- Primary representative to OHLS/PCC and NSC/PCC subgroups, CIAO Council, and CIPIS
- Develops strategies to support OSD CIP requirements

J-6 Cyber/Information

- Coordinates IA and Network Operations issues
- Coordinates with advisory groups to Integrate DIAP into CIP program
- Primary interface with GIG sector
- Addresses CIP IA issues in CJCSI, and checklists (MNSs, GRDs, ORDs, C4ISPs)

J-7 Doctrine/Training

- Lead for coordinating JSCP with J-5 and JPEC for CIP issues
- Reviews CIP standards for compliance
- Lead for support to the CCs in the development of Appendix 16 to Annex C to their OPLANS
- Coordinates with J-7 on Joint Task Lists

J-8 Requirements/ Budget/ Exercises

- Lead for coordinating PPBES issues and reviewing adequacy or resources
- Conducts strategic analysis as directed by JROC
- Assists J-3 in review of critical vulnerabilities list
- Tracks CIP requirements reflected in IPLs and advises CC CIP representatives on resource process

The draft DOD Directive and Instruction 3020 require that the Chairman, Joint Chiefs of Staff support the following CIP functions:

Key Functions:

- Ensure that Critical Infrastructure Protection is fully integrated into the deliberate and crisis action planning processes.(J3/J5/J7)
- Assist the Combatant Commanders in identifying infrastructure assets that are critical to the execution of the National Military Strategy.(J3)
- Prepare joint doctrine for the Department's Critical Infrastructure Protection Program.(J7)
- Validate and prioritize the Combatant Commanders' lists of critical infrastructure assets and related vulnerabilities.(J3, J5, J8)
- Assess the adequacy of Service resources dedicated to redress Critical Infrastructure Protection related vulnerabilities.(J8)
- Ensure Critical Infrastructure Protection issues are incorporated in Joint Exercises.(J8)
- Ensure Critical Infrastructure Protection issues are addressed in National Defense University professional education programs.(J7)
- Provide military advice to the Secretary of Defense on the identification and resource prioritization for critical assets necessary to execute the National Military Strategy.(J8)

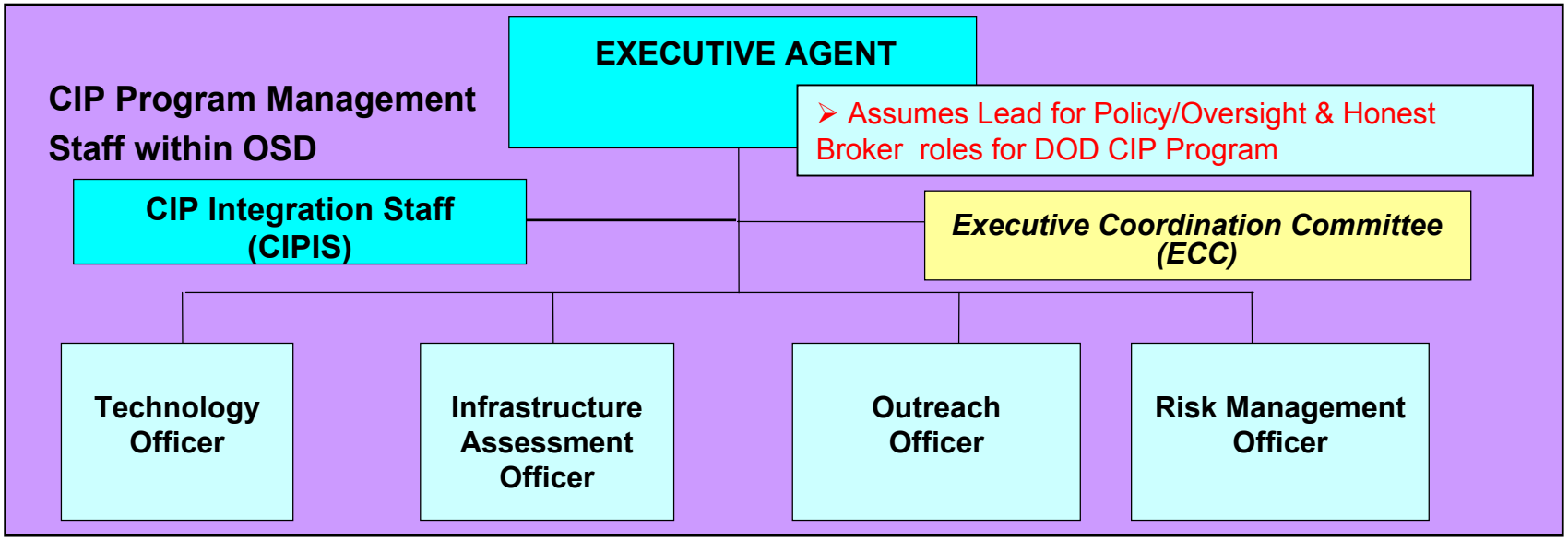
By adopting the recommended key roles and engaging in the recommended functions, the DOD CIP Program will be better positioned to...

- Provide a single focal point within the Department of Defense to reduce redundancy and confusion in the DOD CIP arena
- Establish the mechanism for DoD to share CIP related information with the Intelligence Community, other Government agencies, and private sector components as needed
- Leverage the security resources of both the Government and industry
- Provide enhanced global visibility to improve stakeholder understanding and to protect the Defense Infrastructure
- Move the DOD CIP arena closer toward a desired future state.

Program Management Options

1. **Option 1:** Formal Designation of an Executive Agent and creation of a CIP Program Management Office within OSD
2. **Option2:** Creation of a DOD CIP Field Activity (CIPFA)
3. **Option 3:** Designation of an Office of Primary Responsibility (OPR) for Mission Assurance/CIP within the Joint Staff
4. **Option 4:** Combination of Options 1,2 and 3

Option 1: Formal Designation of an Executive Agent and creation of a CIP Program Management Office within OSD



➢Appoint Technical Direction Agent
- R&D
- Standards
- Tools

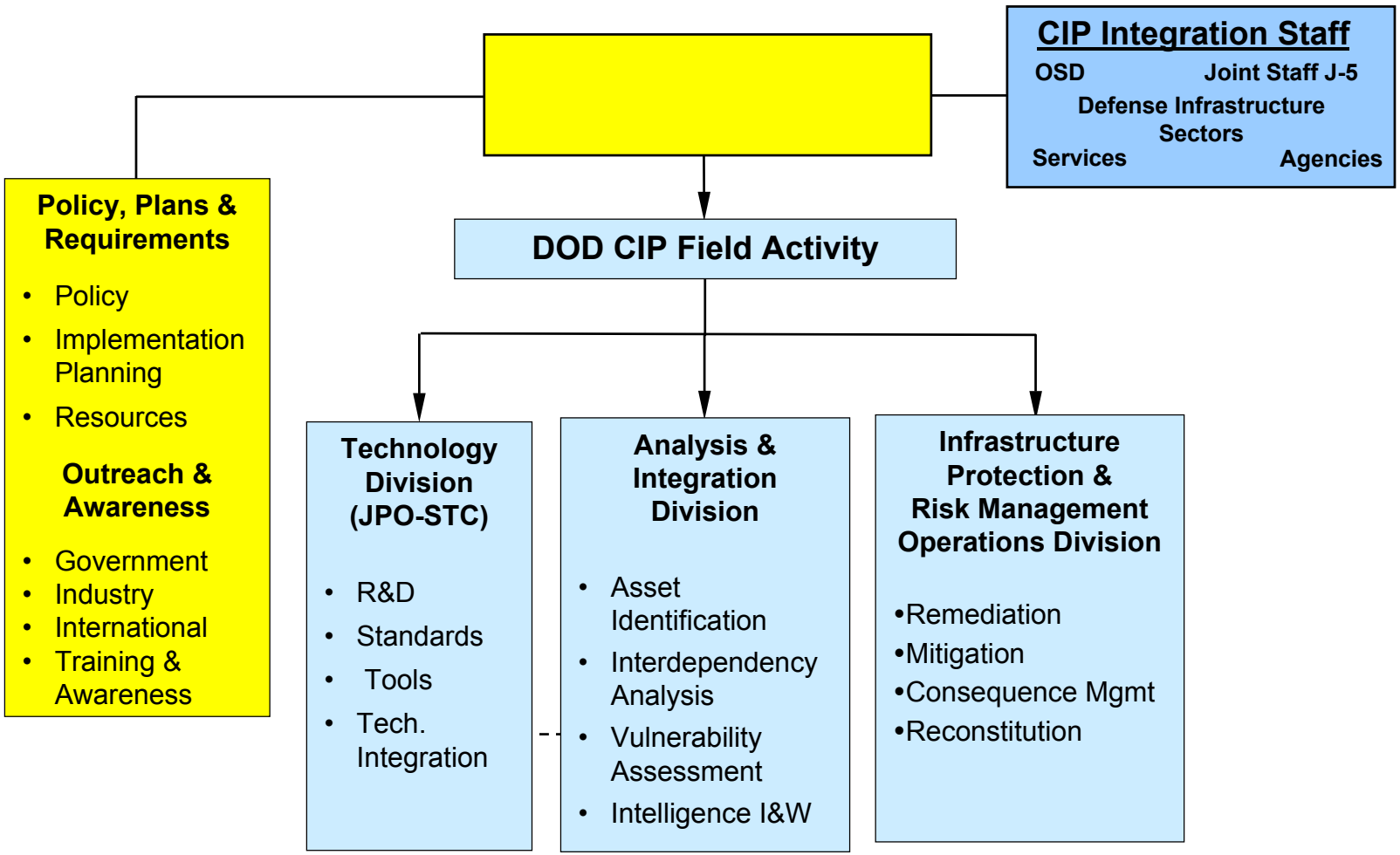
➢Appoint Lead for Analysis and Integration
- Asset Identification
- Interdependency Analysis
- Vulnerability Assessment
- Intelligence I&W

➢Appoint Lead for Outreach
- Government
- Industry
- International
- Training & Awareness

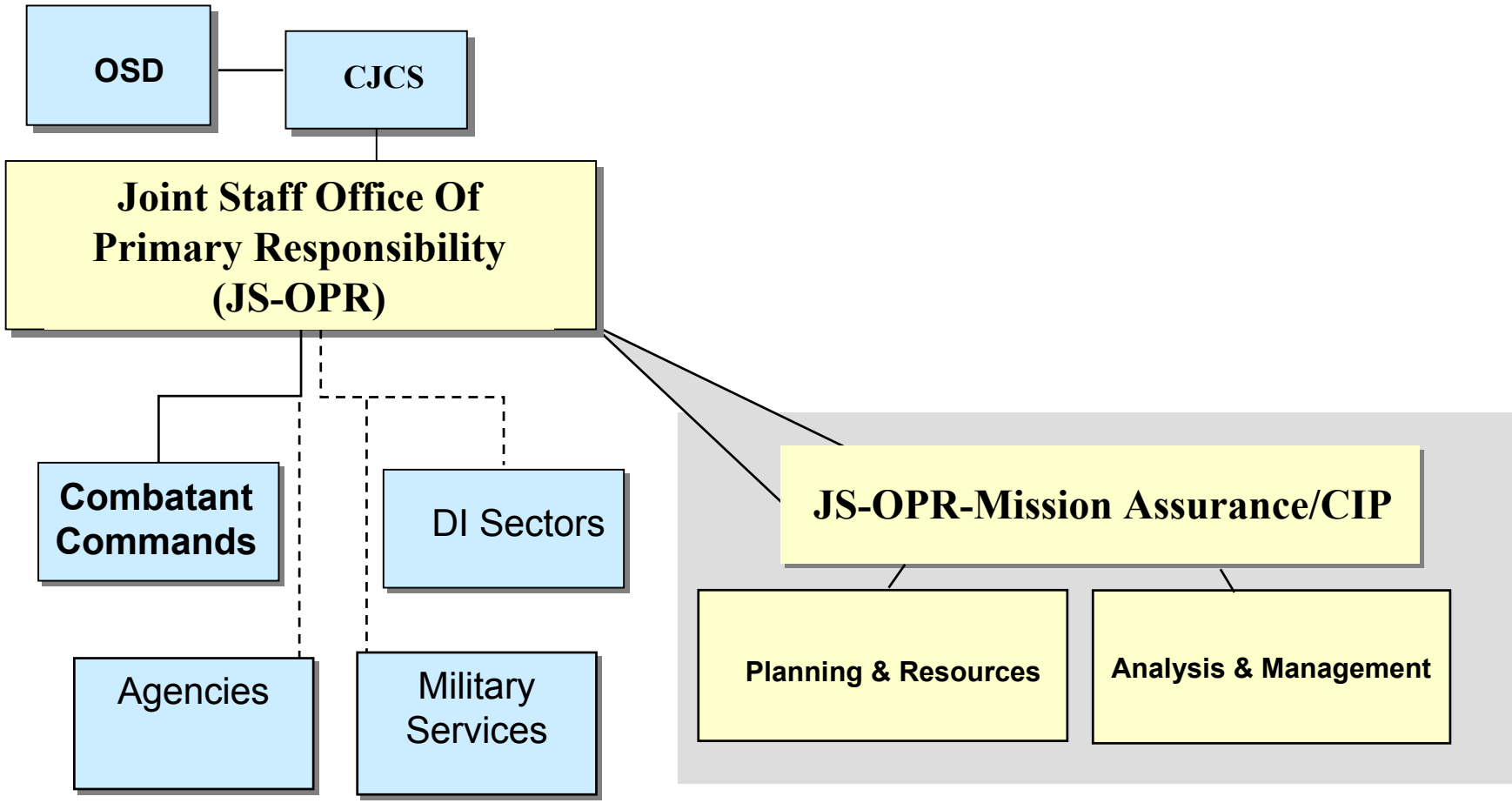
➢Appoint Lead for Risk Management
- Remediation
- Mitigation
- Response
- Reconstitution

- ***The distribution of roles enhances cross-organizational ownership of the DOD CIP mission.***
- ***The CIPIS and ECC provide the mechanism for cross-division coordination of roles.***

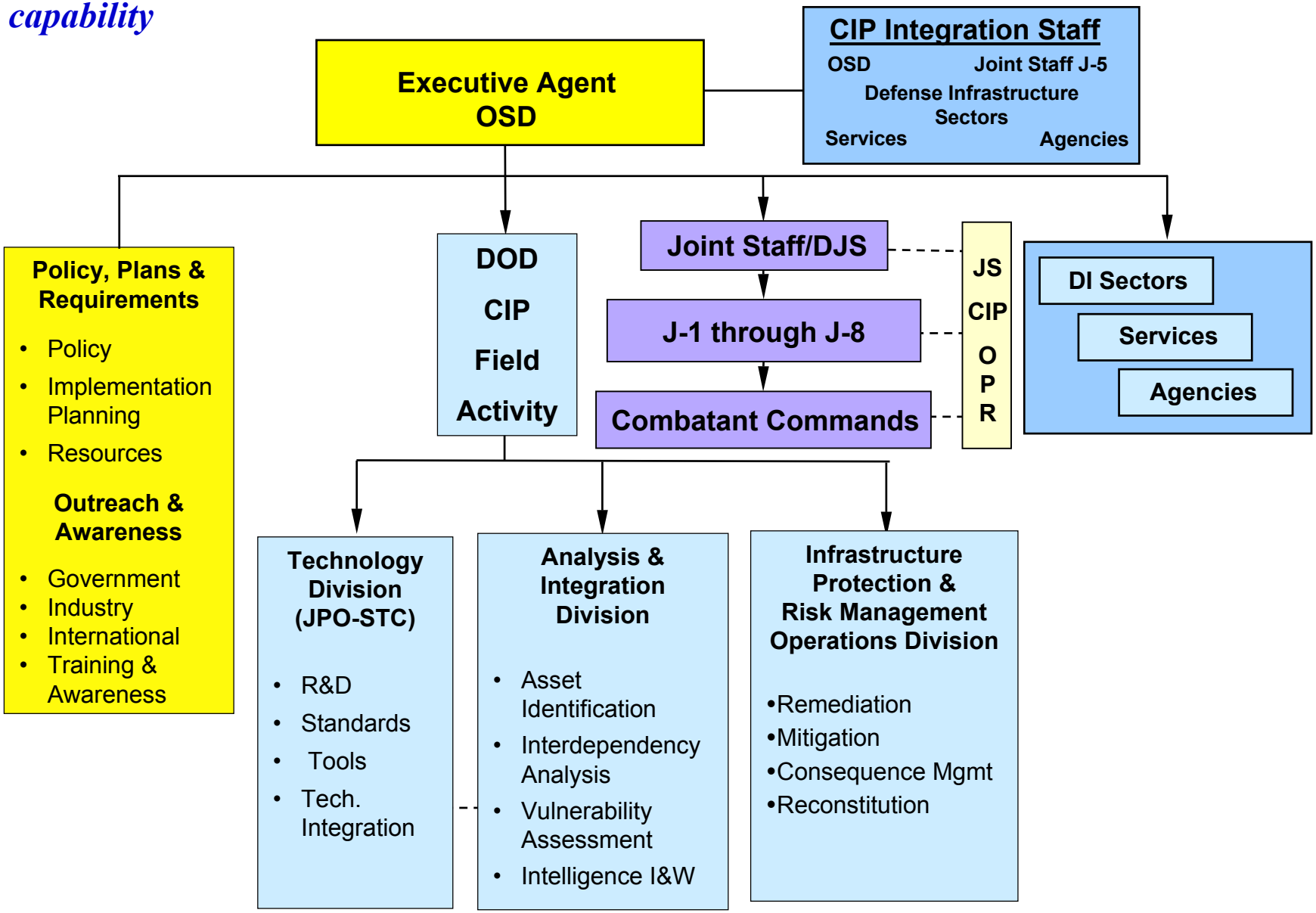
Option 2: Creation of a DOD CIP Field Activity (CIPFA)



Option 3: Designation of a Joint Staff OPR for Mission Assurance and CIP



Option 4: Combination of Options 1,2 and 3 -- a fully integrated risk management capability



The CIP program will benefit by streamlining its current business processes through enhanced development of:

- **A results-oriented, risk management framework** that supports the implementation of CIP policies across DOD
- **A strategic plan** that clearly defines the programs overall purpose, mission and intent to meet emerging and future challenges
- **A performance plan** that describes detailed implementation actions and measurement of performance**.**
- **A streamlined, structured approach** that supports the analysis and assessment of critical infrastructures, threats and vulnerabilities
- **A risk-based decision-making process** for recommending allocation of resources for the protection of critical infrastructures assets
- **A communication strategy** for CIP stakeholders to increase the opportunity for information sharing and overall program success

BACK-UP SLIDES

The following references were reviewed and integrated into the findings of this study.

YEAR	TITLE	SOURCE
2003	Draft DoD CIP Directive	DODD 3020
2003	Draft DoD CIP Instruction	DODI 3020
2003	Draft Chairman, Joint Chiefs of Staff Instruction for CIP	CJCSI 3209.01
2002	DOD CIP Strategy	ASD/C3I
2002	DOD CIP 2002 Executive Report	OASD
2002	National Security Strategy for the Physical Protection of Critical Infrastructures and Key Assets	White House, Office of Homeland Security
2002	National Cyber Security Strategy	White House, Office of Homeland Security
2001	J34 Memorandum of Agreement for JS Integrated Vulnerability Assessment Support	JS (J34)
1988	Assignment of Emergency Preparedness Responsibilities	Executive Order 12656
1996	Critical Infrastructure Protection [established President's Commission on Critical Infrastructure Protection (PCCIP)	Executive Order 13010
1998	Presidential Directive, CIP	PDD63
1998	CAAP	DODD 5160.54
1998	DOD CIP Plan	ASD/C3I
1997	Various Reports on Critical Infrastructure Protection, Force Protection and Information Assurance	U. S. General Accounting Office Reports

Additional responsibilities from DODI 3020 will be assigned to the Joint Staff functional areas.

J-1
Personnel

- Ensure a sufficient number of adequately trained personnel are available to execute the DoD Critical Infrastructure Protection Program.

Additional responsibilities from DODI 3020 will be assigned to the Joint Staff functional areas.

J-2
Intelligence/I&W

- Establish Department-wide information classification, release, and special handling instructions for the DoD Critical Infrastructure Protection Program.
- Ensure relevant legal issues, as well as proprietary protection, counterintelligence, and law enforcement issues are addressed fully in support of DoD Critical Infrastructure Protection Program goals and objectives.
- Ensure present and projected indications and warning networks are used to submit operational status reports on the viability of every identified critical infrastructure asset and their interdependent potential points of failure.
- Lead development of I&W methodology for DoD CIP.
- Coordinate threat intelligence support to DoD sectors, commands, services, and agencies.
- Ensure that threat assessments on DoD infrastructures, systems, or assets are prepared and presented to appropriate CIP stakeholders.
- In cooperation with the Counterintelligence Field Activity (CIFA), provide counter-intelligence support to the CIP leadership and organizations, in coordination with the Military Services.
- Coordinate all-source analysis and data fusion to generate CIP alerts and warnings for on-going events.
- Contribute to identification of requirements and development of I&W predictive analysis tools.
- Interface between government and industry to promote the sharing of classified information in a protected and trusted environment.

Additional responsibilities from DODI 3020 will be assigned to the Joint Staff functional areas.

J-3
Operations

- Assist the Combatant Commanders in identifying infrastructure assets that are critical to the execution of the National Military Strategy.
- Oversee application of a standard methodology for identifying the critical domestic and foreign infrastructure assets the Department relies upon to fulfill its homeland defense and force projection responsibilities.
- Oversee development and maintenance of a distributed database that will serve as the master DoD repository for all critical infrastructure asset and interdependency related information.
- Provide guidance on and maintain cognizance of DoD Critical Infrastructure Protection Program related mitigation and remediation activities.
- Develop a standard, customer friendly methodology for identifying the critical domestic and foreign infrastructure assets the Department relies upon to fulfill its homeland defense and force projection responsibilities.
- Develop analytical standards and procedures to permit effective, Department-wide, infrastructure support analyses and vulnerability assessments.
- Develop capability to provide the Secretary of Defense, Chairman of the Joint Chiefs of Staff, Military Departments, and Combatant Commands real time situational awareness of infrastructure assets designated as critical to U.S. military operations.
- Provide a framework that will enable DoD to monitor and manage the readiness posture of mission essential components of the critical infrastructures that D0D relies on.
- Provide guidance on and maintain cognizance of DoD Critical Infrastructure Protection Program related risk mitigation and remediation, response and reconstitution activities.
- Validate and prioritize the Combatant Commanders' lists of critical infrastructure assets and related vulnerabilities.

Additional responsibilities from DODI 3020 will be assigned to the Joint Staff functional areas.

J-3
Operations
(Continued)

- Coordination with the appropriate DoD Components and with the permission of the owners, physical vulnerability assessments of designated DoD and non-DoD classified and unclassified critical infrastructures.
- Identify and map the interdependencies across all the critical infrastructures.
- Identify single points of failure across all relevant critical infrastructures.

Additional responsibilities from DODI 3020 will be assigned to the Joint Staff functional areas.

J-4
Logistics

- Work with the Under Secretary of Defense for Acquisition, Technology, and Logistics, to ensure its policies and assurance standards established as a result of Draft DoD Directive 3020 are integrated into all appropriate acquisition policy guidance.
- In conjunction with the DHS and the DOS, facilitate the sharing of industry's sensitive information with the Government in a protected and trusted environment.

Additional responsibilities from DODI 3020 will be assigned to the Joint Staff functional areas.

J-5
Policy & Strategy

- Oversee development and implementation of DOD Directives and Instructions for CIP throughout the Department to ensure all DoD Components are complying.
- Conduct an annual review of the DoD Critical Infrastructure Protection Program to ensure the Department is meeting its goals and objectives.
- Ensure effective physical and cyber vulnerability assessment policies and procedures are developed and implemented fully throughout the Department.
- Develop CIP input to the Defense Planning Guidance (DPG).
- Work with DHS to establish a dialogue throughout the Federal and State governments to foster a common understanding of the interagency interdependencies.
- In conjunction with the Department of Homeland Security (DHS) and the Department of State (DOS), elevate the awareness of and promote Critical Infrastructure Protection through a variety of activities, such as information sharing and cooperative agreements with the private sector, as well as other federal departments, state and local governments, and allied/friendly foreign governments as applicable.
- Represent the DoD in Critical Infrastructure Protection related discussions and agreements with other U.S. Government, private sector officials, state and local governments, and allied/friendly foreign governments.
- Develop relationships with Federal departments and agencies identified in Draft DOD Directive 3020.
- Facilitate cooperation and sharing of tools, techniques, and lessons learned across the Sectors, Commands, Services and Agencies.

Additional responsibilities from DODI 3020 will be assigned to the Joint Staff functional areas.

J-6
Cyber/Information

- Work with the Director, Defense Information Systems Agency to develop and maintain a network that allows real-time alerts and warnings CIP-wide, and that facilitates the routine sharing of information concerning risks to critical infrastructures.
- Work with the Director, National Imagery and Mapping Agency to support the DoD Critical Infrastructure Protection Program with the annotated imagery needed for the development of situational awareness and complex modeling and simulation visualization tools.
- Contribute to identification of requirements and development of I&W predictive analysis tools.
- Work with the Director, National Security Agency to conduct or oversee, in coordination with the appropriate DoD Components and with the permission of the owners, cyber vulnerability assessments of designated DoD and non-DoD classified critical infrastructure assets. Require the Director, National Security Agency to conduct or oversee all actions that are necessary to increase the reliability, redundancy, protection, and restoration of classified information systems supporting DoD critical infrastructure assets.(Source: Draft DODD 3020)
- Work with the Director, Defense Information Systems Agency to conduct or oversee all actions that are necessary to increase the reliability, redundancy, protection, and restoration of unclassified information systems supporting DoD critical infrastructure assets.
- Facilitate emergency response planning, training and exercises across all sectors.

Additional responsibilities from DODI 3020 will be assigned to the Joint Staff functional areas.

J-7
Doctrine/Training/Conventional War Plans

- Ensure that Critical Infrastructure Protection is fully integrated into the deliberate and crisis action planning processes.
- Prepare joint doctrine for the Department's Critical Infrastructure Protection Program.
- Oversee the Department's Critical Infrastructure Protection related training and awareness program initiatives.

Additional responsibilities from DODI 3020 will be assigned to the Joint Staff functional areas.

J-8
Requirements/Budget/Exercises

- Ensure the Critical Infrastructure Protection Program is incorporated into the DoD Planning, Programming, Budgeting & Execution System (PPBES) process.
- Develop and maintain the CIP financial baseline.
- Develop Program Objective Memorandum (POM) analysis process to streamline DoD CIP PPBES Programming Phase processes, enable collaborative development, adequately characterize requirements and balance resources across the DOD CIP enterprise in real time IAW planning guidance.
- Implement common Work Breakdown Structure (WBS) and Financial Management (FM) tool set to capture, understand and control cost and enable automated linkage of the POM and Budgeting Phases. Implement financial and cost metrics to measure performance against benchmarks.
- Perform analyses of DOD CIP POM requirements, capabilities and resources to develop set of POM issues that efficiently resource existing DoD CIP program requirements and suitably justify unfunded items.
- Develop budget issues and perform trend analysis for the DoD CIP Program in support of OSD and President's Budget Estimate Submission development.
- Recommend alternative mechanisms for funding DoD CIP initiatives which benefit multiple Federal departments, agencies, and entities.
- Identify appropriate levels of funding for budget submissions to support DoD CIP requirements.